VERIFICATION OF TRANSLATION

I, Minoru KUDOH
of a citizen of Japan residing at: 406, 17-15,
Minamiooi 1-chome, Shinagawa-ku, Tokyo 140, Japan
certify that I am familiar with the English and Japanese languages, and to the best of my knowledge and belief the following is a true translation of the officially certified copy of the Japanese Patent Application, Heisei 11-098140.

This 9 day of June, 2004

Minoru KUDOH

[Document Name] PATENT APPLICATION

[Identification No.] 47201392

[To] Commissioner; Japanese Patent Office

[International Patent Classification] H04L 9/00
H04L 12/00

[Inventor]

[Domicile or Residence] c/o NEC Corporation, 7-1, Shiba 5-chome, Minato-ku, Tokyo, Japan

[Name] Jun KAMETANI

[Applicant]

[ID number] 000004237

[Name] NEC Corporation

[Attorney]

[ID number] 100093595

[Patent Attorney]

[Name or Title] Masao MATSUMOTO

[Indication of Charge]

[Deposit Payment Register Number] 057794

[Amount of Fee] 21000 yen

[Items of the Filing Articles]

[Article Name] Specification one copy

[Article Name] Drawings one copy

[Article Name] Abstract one copy

[General Power of Attorney] 9803702

[Proof] NECESSARY

[Document Name] Specification

[Title of the invention] PACKET SWITCHING APPARATUS

[Scope of Patent to be Claimed]

[Claim 1]

A packet switching apparatus used in a packet communication to transfer a packet, which carries out a routing process in a packet, characterized in including:

a microprocessor which carries out routing process for a received packet under software program control;

an IP flow table which registers and stores a result of said routing process as for a packet, to which said routing process is carried out by said microprocessor, using an IP source address and an IP destination address as a search key;

a means for packet process which

searches said IP flow table using said IP source address and said IP destination address as a search key at receiving a packet, and

which transfers said packet to an appropriate output port based on a result of a routing process indicated by said IP flow table without carrying out routing process by said microprocessor when a result of said searching indicates that a corresponding IP flow;

a means for lower layer process which are connected to a network interface, and

carries out a lower layer process for a received packet to be transferred to said means for packet process, and

carries out a lower layer process for a received packet from said means for packet process to be outputted to a network.

[Claim 2]

A packet switching apparatus according to claim 1 characterized in further including a means for security to carry out an encryption process and a decryption process for a packet by an exclusive hardware, wherein

said microprocessor determines an encryption or decryption algorism and an encryption key as security data when said microprocessor judges that a packet should be encrypted or decrypted based on a predetermined rule and notifies said security data to said means for security; and

said means for security carries out an encryption process or a decryption process of packets based on said security data received from said micro processor.

[Claim 3]

A packet switching apparatus according to claim 1 which is characterized in that;

said IP flow table registers said security data determined by said microprocessor in additional to said result of routing process;

said means for packet process sends said received packet to said means for security process together with said security data indicated in said IP flow without entering into a step of gaining said security data by said microprocessor, when a corresponding IP flow is registered and said security data is registered onto said IP flow entry as a result of searching said

IP flow table using a IP resource address and a IP destination address of said received packet as a search key; and

said means for security process carries out a encryption process and a decryption process for a packet based on a security data received from said means for packet process.

[Claim 4]

A packet switching apparatus according to Claim 2 or Claim 3 characterized in that;

said microprocessor and said means for packet process are connected each other through a processor bus;

said means for packet process and said means for lower layer process are connected each other through a predetermined switch fabric; and

said means for security process is connected with a switch fabric same as a switch fabric of said means for lower layer process.

[Claim 5]

A packet switching apparatus according to Claim 2 or Claim 3 characterized in that said means for packet process encapsulates a packet which is encrypted by said means for security process as a communication packet used in communication between a packet apparatus for destination of said packet.

[Claim 6]

A packet switching apparatus used in packet communication network to transfer a packet, which carries out a routing process in a packet unit, characterized in including:

a microprocessor carries out a routing process for a received

packet under an software programs;

a means for security process carries out an encryption and a decryption of packets by an exclusive hardware;

a means for lower layer process connected with a network interface, which carries out a lower layer process to a packet received and a packet to be transmitted, together with carrying out transmitting and receiving of a packet ,wherein

said microprocessor determines an encryption key and an algorism for encryption and decryption as a security data when a packet should be judged to be encrypted and decrypted based on a predetermined rule, and notifies said determination to said means for security process; and

said means for security process carried out an encryption and a decryption of a packet based on a security data received from said microprocessor.

[Claim 7]

A packet switching apparatus according to Claim 6 characterized in that said microprocessor and said means for lower layer process are connected with a switch fabric same as a switch fabric of said means for lower layer process.

[Detailed Description of the Invention]

[0001]

[Technical Field to which the Invention belongs]

The present invention relates to packet switching apparatus used in a packet communication network, especially, relates to the packet switching apparatus to reduce a load of a

microprocessor and to fasten a routing process speed.

[0002]

[Conventional Technique]

In a packet communication network which is represented by the Internet, the transmission of data is carried out in a packet unit. The packet contains the header which contains a source address and a destination address of the packet data. A packet switching apparatus such as a router transfers the packet in the packet unit to an appropriate destination at the network based on the destination address of the header.

[0003]

Conventionally, the packet routing process is carried out in a packet unit and is generally carried out as a software based process.

Fig. 9 shows a block diagram showing the structure of a conventional example of the packet switching apparatus for carrying out the packet routing process.

The packet switching apparatus shown in Fig. 1 is configured by a microprocessor 101, a main memory 102, a packet memory 105, lower layer processing sections 110 and a DMA controller 112. The main memory 102 stores a software program executed on the microprocessor 101 and routing data. The packet memory 105 stores received packets. Each of the lower layer processing sections 110 has the hardware structure which executes the processes for a data link layer and a physical layer. The DMA controller 112 transfers the packet between the lower layer processing section 110 and the packet memory 105.

[0004]

In a conventional router which has the structure shown in Fig. 9, when a packet is received, the DMA controller 112 transfers the received packet from the lower layer processing section 110 to the packet memory 105 once. After this, the microprocessor 101 copies the packet stored in the packet memory 105 in the main memory 102 via a processor bus 103. Then, a routing process is carried out under the software control. The packet which header is replaced with a MAC header by the process is again copied into the packet memory 105.

Next, the DMA controller 112 transfers the processed packet to the lower layer processing sections 110 connected with a physical output port. The lower layer processing section 110 transmits the transferred packet to a network after its process.

[0005]

As described above, in the conventional example of the packet switching apparatus, the routing process to all packets is carried out by the microprocessor 101 under the software control. Therefore, the network speed depends on the performance of the microprocessor 101 itself.

[0006]

By the way, as for the packet communication method, it is conventionally pointed out that the security of data is weak compared with a line switching system.

Also, with the rapid spread of the Internet in recent years, the data security in the packet communication is an urgent problem.

For this reasons, the system for encrypting IP packet data (or IPsec) is standardized as the security measure in the network layer. In the conventional packet switching apparatus, all of the processes of encrypting and decrypting for a packet data based on the IPsec are carried out by the microprocessor 101.

[0007]

[Problems the Invention Tries to Solve]

As mentioned above, in the conventional packet switching apparatus, all of routing processes for the received packet are carried out by the microprocessor 101 under the software, so that the communication speed in the network depends on the performance of the microprocessor itself.

Therefore, as for countermeasure for the increase of the communication traffic and the increase of the network speed, the limit of the performance of the microprocessor is a matter of dispute.

[0008]

In the packet switching apparatus shown in Fig. 9, if the packet memory 105 and the main memory 102 are formed in a same memory device as a unit, the time which is necessary for the data transfer between the memories can be reduced. However, the problem still remained so far as the limit of the performance of the microprocessor because all the processes for every packet are the loads for the microprocessor.

[0009]

Also, the conventional packet switching apparatus may supports a encrypting and decrypting process for the packet based on the

above-mentioned IPsec in order to improve security of the packet communication.

In this case, the performance microprocessor is interrupted for executing the encrypting and decrypting process. This causes a decreasing of the whole processing efficiency for the packet switching apparatus and a decreasing of performance limit to correspond the high processing speed.

[0010]

More specifically, when the IPsec processing is newly added to the above mentioned conventional packet switching apparatus, the data throughput of the packet sometimes fell to about 1/10.

[0011]

An object of the present invention is provide a packet switching apparatus to achieve a high speed packet switching process by reducing the load of a microprocessor at the routing process and the security process.

[0012]

[Means for Solving the Problems]

The present invention used in a packet communication to transfer a packet, which carries out a routing process in a packet, characterized in including; a microprocessor which carries out routing process for a received packet under software program control; an IP flow table which registers and stores a result of the routing process as for a packet, to which the routing process is carried out by the microprocessor, using an IP source address and an IP destination address as a search key;

a means for packet process which searches the IP flow table using the IP source address and the IP destination address as a search key at receiving a packet, and which transfers the packet to an appropriate output port based on a result of a routing process indicated by the IP flow table without carrying out routing process by the microprocessor when a result of the searching indicates that a corresponding IP flow;
a means for lower layer process which are connected to a network interface, and carries out a lower layer process for a received packet to be transferred to the means for packet process, and carries out a lower layer process for a received packet from the means for packet process to be outputted to a network.

[0013]

A packet switching apparatus of the present invention described in claim 2 is characterized in further including a means for security to carry out an encryption process and a decryption process for a packet by an exclusive hardware, wherein the microprocessor determines an encryption or decryption algorism and an encryption key as security data when the microprocessor judges that a packet should be encrypted or decrypted based on a predetermined rule and notifies the security data to the means for security; and the means for security carries out an encryption process or a decryption process of packets based on the security data received from the micro processor.

[0014]

A packet switching apparatus of the present invention

described in claim 3 is characterized in that; the IP flow table registers the security data determined by the microprocessor in additional to the result of routing process; the means for packet process sends the received packet to the means for security process together with the security data indicated in the IP flow without entering into a step of gaining the security data by the microprocessor, when a corresponding IP flow is registered and the security data is registered onto the IP flow entry as a result of searching the IP flow table using a IP resource address and a IP destination address of the received packet as a search key; and the means for security process carries out a encryption process and a decryption process for a packet based on a security data received from the means for packet process.

[0015]

A packet switching apparatus of the present invention described in claim 4 is characterized in that; the microprocessor and the means for packet process are connected each other through a processor bus; the means for packet process and the means for lower layer process are connected each other through a predetermined switch fabric; and the means for security process is connected with a switch fabric same as a switch fabric of the means for lower layer process.

[0016]

A packet switching apparatus of the present invention described in claim 5 is characterized in that the means for packet process encapsulates a packet which is encrypted by the

means for security process as a communication packet used in communication between a packet apparatus for destination of the packet.

[0017]

A packet switching apparatus of the present invention described in claim 6 used in packet communication network to transfer a packet, which carries out a routing process in a packet unit, is characterized in including: a microprocessor carries out a routing process for a received packet under an software programs; a means for security process carries out an encryption and a decryption of packets by an exclusive hardware; a means for lower layer process connected with a network interface, which carries out a lower layer process to a packet received and a packet to be transmitted, together with carrying out transmitting and receiving of a packet ,wherein the microprocessor determines an encryption key and an algorism for encryption and decryption as a security data when a packet should be judged to be encrypted and decrypted based on a predetermined rule, and notifies the determination to the means for security process; and the means for security process carried out an encryption and a decryption of a packet based on a security data received from the microprocessor.

[0018]

A packet switching apparatus of the present invention described in claim 7 is characterized in that the microprocessor and the means for lower layer process are connected with a switch fabric same as a switch fabric of the means for lower

layer process.

[0019]

[Embodiments of the Invention]

Hereinafter, an embodiment of the present invention will be described below in detail with reference to the attached drawings.

[0020]

Fig. 1 is a block diagram showing a structure of the packet switching apparatus according to an embodiment of the present invention.

Referring to Fig. 1, the packet switching apparatus in the embodiment is constituted by a microprocessor 11, a main memory 12, a processor bus 13 to connect each other parts, a packet processing section 14 to execute a packet process in place of the microprocessor 11, a packet memory 15, a search processing section 16, an IP flow table 17, a security processing section 19 to execute a encryption/decryption process and a lower layer processing sections 20, a switch fabric 18 to connect the lower layer processing section 20, the packet processing section 14, the security processing section 19 and the lower layer and processing section 20 mutually.

It should be noted that only the structure part characterized by the present invention is shown in Fig. 1,and the other general structure parts are omitted.

[0021]

In the above structure part, the microprocessor 11 executes not only a software program control to control the whole packet

switching apparatus but also carries out a routing process to determine the transmitting destination of a received packet, and also executes determining process to determine the necessity of the encrypting or decrypting process for the received packet.

[0022]

The main memory 12 stores the software program to control the microprocessor 11 and various kinds of data related to predetermined processes.

[0023]

The packet processing section 14 carries out such processes onto the packet received via network interfaces as an IP header process and a transferring process to a network interface to be transferred.

Here, the IP header process includes various processes, such as an extracting process wherein an IP destination address and an IP source address are extracted from the header added to the received packet, and a generating process wherein a new MAC header is generated in accordance with a MAC address which is determined through the routing process by the microprocessor 11.

[0024]

The packet processing section 14 controls the search processing section 16 by a search key extracted from the packet header in order to search the IP flow table or register tentatively a new IP flow to the IP flow table 17.

Also, the packet processing section 14 carries out the IP header process based on an acquired physical output port and a MAC address corresponding to the search result of the IP flow

table 17 by the search processing section 16.

[0025]

The packet memory 15 temporarily stores the received packet for the processing by the microprocessor 11 and the packet processing section 14.

Also, the packet memory 15 has a processing queue in which the received packets are registered as waiting the result of the routing process by the microprocessor 11.

[0026]

The search processing section 16 searches the IP flow table 17 in response to the instruction from the packet processing section 14 and replies a result of the routing process of the packet to the packet processing section 14.

Also, in case the IP flow corresponding to the instruction from the packet processing section 14 does not exist, the search processing section 16 carries out a tentative registration of the IP flow based on the instruction from the packet processing section 14. The search processing section 16 stores the received result of the routing process by the microprocessor to the IP flow entry as a tentative registration and then, the IP flow is registered determinately.

[0027]

The IP flow table 17 is a table for storing the IP flow as a result of the routing process by the microprocessor 11, using an IP source address and an IP destination address as a search key.

Fig. 2 shows an example of IP the flow table 17. Referring to Fig. 2, in the IP flow table 17, the IP source address and the

IP destination address as the search key, the MAC source address as the result of the routing process, the MAC destination address, and a port number of the physical output port, are registered in every IP flow entry. Also, if needed, a security data described follow is stored in the IP flow table.

[0028]

The switch fabric 18 mutually connects between the plurality of lower layer processing sections 20 which are respectively connected with a plurality of network interfaces, the packet processing section 14 and the security processing section 19. The switch fabric 18 may be any kind of circuit if the circuit has an arbitration function and an addressing function for the data transferring between each connected sections. Also, the means for the function may be any kind of bus or the like, such as a simple tri-state bus, a ring bus, or a crossbar switch. Further, the switch fabric 18 may be formed to have a token ring bus structure.

[0029]

The security processing section 19 carries out the encrypting process and the decrypting process for every packet as an occasion demands on the basis of the software processing by microprocessor.

[0030]

The lower layer processing sections 20 is connected with the physical network interface to carry out the processing of a data link layer (the second layer of the OSI7 layer model) and a processing of the lower layer, then carries out the transmission

and reception of the packet with the packet processing sections 14 through the switch fabric 18.

[0031]

As described up to this, a structure of the present invention according to the embodiment, but actually, the packet switching apparatus in the embodiment may be attained by various circuits which realize the functions of the above components. For example, a semiconductor integrated circuit which includes the above mentioned components may configure the packet switching apparatus of the present invention

[0032]

Next, the operation of the packet switching apparatus in the embodiment will be described below in detail with each flow chart shown in Fig.3 to Fig. 7.

Fig. 3 is a flow chart showing a main flow of a packet process in the embodiment.

Fig. 4 is a flow chart showing a flow of the routing process by the microprocessor 11.

Fig. 5 to Fig.7 show flows of the packet processes in the embodiment adding the security process.

[0033]

The packet switching apparatus of the embodiment carries out the process of a network layer of the packet communication which is represented by the Internet. Therefore, the header of a packet received from a network interface is analyzed and the routing process is carried out based on the destination address (an IP destination address). According to the result of the

process, the packet is transferred to the network interface as an out putting destination. These processes are the basic operation of the packet switching apparatus.

Additionally, in another embodiment of the present invention, the security process such as the encrypting/ decrypting of the data is executed in every packet based on the IP destination address and the IP resource address during the routing process of the reception packet as occasions demand.

Now, in the following description of the operations, a normal operation without security process is explained earlier, and the operation with the security process follows.

[0034]

Referring to Fig. 3, firstly, an IP packet arrives from an external apparatus at the lower layer processing sections 20 of the packet switching apparatus which is connected with an external network (Step 301).

Next, the lower layer processing section 20 carries out the packet process of a layer 2 and following processes, that is a synchronous establishing process of data, a verifying process of a lower layer header (such as a MAC header), and a calculating process of CRC (Step 302).

Then, the packet, which the processing in the lower layer is executed, is transferred to the packet processing section 14 via the switch fabric 18.

[0035]

The packet processing section 14 receives the transferred reception packet to store in the packet memory 15. After that,

the packet processing section 14 extracts the IP destination address and the IP source address from the packet header of the packet. Then, the packet processing section 14 generates a search key to search the IP flow table 17 in response to this extraction (Step 303).

Next, the packet processing section 14 sends out the generated search key to the search processing section 16 in order to instruct the search for the IP flow table 17

[0036]

The search processing section 16 carries out the searching for the IP flow table 17 using the search key received from the packet processing section 14. The search processing section 16 notifies the search result to the packet processing section 14 (Step 304). As the result of the searching by the search processing section 16, when the IP flow corresponding to the search key is registered on the IP flow table 17, that is, when the microprocessor 11 has already carried out the routing process to the packet corresponding to the IP flow table 17, the packet processing section 14 receives the search result from the search processing section 16. (The search result includes the MAC resource address, the MAC destination address and the port number of the physical output port in the IP flow table 17 shown in Fig. 2.) Then, based on the search result, the packet processing section 14 carries out a header processing (Step 305, 306).

After that, the packet processing section 14 transfers the packet to the lower layer processing section 20 which is

connected with the physical output port as indicated by the mentioned search result (Step 307).

In this way through the above processes, the packet can be transferred automatically without any routing process of the microprocessor 11 under the software control.

[0037]

The lower layer processing section 20 receives the packet from the packet processing section 14 through the switch fabric 18, and then carries out the processing peculiar to the lower layers (Step 308), that is, carries out CRC calculation of the whole packet and a process of adding a calculation result to the packet. Then, the lower layer processing section 20 sends out the packet to the connected network interface (Step 309).

[0038]

On the other hand, as the result of the searching by the search processing section 16, when the IP flow corresponding to the search key is not registered on the IP flow table 17, the packet processing section 14 instructs the search processing section 16 to carry out a tentative registration of a new IP flow, which search key is the IP destination address and the IP resource address (Step 305, 310). This case corresponds to the IP flow entry which has only the search key item in the IP flow table of Fig. 2.

Next, the packet processing section 14 interrupts the microprocessor 11 so as to hand the packet over for the routing process (Step 311). At this time, the packet is registered on the processor processing queue of the packet memory 15. After

that, the packet processing section 14 starts the following processing of the packet (Step 312).

[0039]

After this, the packet processing section 14 checks the packets of the processor processing queue of the packet memory 15 during the packet process of the newly received packet. Then, the packet processing section 14 produces a search key of the packet located at the head of the queue. The packet processing section 14 controls the search processing section 16 to carry out the searching operation of the IP flow table 17 (Step 313).

As is will be described later, if the routing process by the micro processor 11 to the packet has completed, the corresponding IP flow is formally registered. Then, the MAC source address, the MAC destination address and the port number of the physical output port are gained as the search result. (Step 314) In this time, the header processing of the packet is carried out by the packet processing section 14 based on the gained MCA address and the port number of the physical output port. (Step 315)

In the following steps, the packet is transmitted to the lower layer processing section 20, the processing peculiar to the lower layer is carried out, and then, sent to the network interface. (Step 307, 308, 309)

[0040]

Even if the packet which has the identical IP resource address and IP destination address is received, the corresponding IP

flow is registered on the IP flow table 17. Therefore, the packet processing section 14 can transfer the packet automatically by the processing of the step 305,306 and 307 without the routing process of the microprocessor 11 by the software control.

[0041]

Next, an operation of the microprocessor 11 when the packet is handed over to the microprocessor 11 for the routing process at the step 311 will be described below.

Referring to Fig. 4, the microprocessor 11 starts the routing process in response to the interrupt from the packet processing section 14. First, the microprocessor 11 accesses the packet memory 15 through the processor bus 13 and the packet processing section 14 (Step 401). The microprocessor 11 copies only the header section of the packet registered on the processing queue of the packet memory 15 into the main memory 12 (Step 402).

[0042]

Next, the microprocessor 11 carries out an searching operation of an IP routing table and an ARP cash table which are previously stored in the main memory 12, using an IP destination address of the copied packet header section as a key (Step 403). Also, the microprocessor 11 determines the physical output port as the destination of the packet and the MAC address of the next hop (Step 404). Further, the microprocessor 11 sends these series of the routing process result to the IP flow table 17 through the processor bus 13 and the search processing section 16 so as to register formally the IP flow entry which has been

tentatively registered (Step 405).

This operation means that the routing result is added into the IP flow entry in the IP flow table 17 of Fig. 2.

[0043]

Hereinafter, the operation in another embodiment of the present invention with a security process in every packet will be described. The security process is explained with an example as a process for IPsec defined IETF (Internet Engineering task Force).

[0044]

When the packet switching apparatus such as a router is supported by IPsec, a method of encapsulating by a communication packet between packet switching apparatuses (tunnel mode) is used. In the method, data such as an encrypting algorithm of a packet and an encryption key are previously shared between the packet switching apparatuses which exist in the network of the destination of the packet.

The encrypting algorithm of the packet and the encryption key are unique between communicating terminal. Therefore, the packet switching apparatus can determine the encrypting algorithm and the encryption key to be applied to the packet from the IP destination address and the IP source address. It is necessary for these sharing data to be established between the packet switching apparatuses previously or depending upon necessity. In this embodiment, all the processing associated with the establishment of the sharing data is carried out by the microprocessor 11 under the software control.

Now, a structure of the IP packet processed in the IPsec tunnel mode is shown in Fig. 8.

[0045]

In the example of the operation, processes to the packet to be handed over for the routing process by the microprocessor 11 from the tentative registration of IP flow onto the IP flow table after the reception of the packet at the packet switching apparatus, is same as the normal process shown in Fig.3. (Refer to Step 301 to 305, 310 and 311)

[0046]

Referring to Fig.5, the microprocessor 11 starts the routing process in response to an interrupt from the packet processing section 14. First, the microprocessor accesses the packet memory 15 through the processor bus 13 and the packet processing section 14 (Step 501). The microprocessor 11 copies only the header section of the packet stored in the processor processing queue of the packet memory 15 into the main memory 12 (Step 502).

[0047]

Next, the microprocessor 11 identifies an IP destination address of the copied packet header section (Step 503). When the packet has the IPsec header shown in Fig. 7 and the IP address is an own address of the packet switching apparatus itself, the microprocessor 11 recognizes the packet as an object to be decrypted by IPsec (Step 504).

When the IP address is not an own address of the packet switching apparatus itself, the microprocessor 11 recognizes the

packet as an object to be encrypted by IPsec (Step 505).

[0048]

Next, referring to Fig. 6, the process of IPsec encrypting object packet will be explained.

In this case, the microprocessor 11 searches tables for the security process (Security Policy Database and Security Association Database) which are previously stored in the main memory 12, using the IP destination address of the packet header section as a key. At this time, the microprocessor 11 determines whether the packet should be encrypted or not (Step 601). When it is determined to be not necessary to encrypt the IP packet, the following processes are the same as the normal processes shown in Fig. 4. That is, the processes such as the process of searching the routing table and the ARP cash table, and the process of registering the search result onto the IP flow table 17 are carried out (Refer to the Steps 403 to 405).

[0049]

When it is determined to be necessary to encrypt the IP packet, the microprocessor 11 sends security data including the encrypting algorithm and the encryption key, an index (SPI) and the like to identify the security data, the IP destination address and the IP resource address of IP packet for encapsulating, to the IP flow table 17 through the search processing section 16 together with the routing data indicating physical port connected to the security processing section 19. Then, the IP flow entry registered tentatively is formally registered. (Step 602)

This operation means that the items of the physical output port and the security data are registered onto the corresponding IP flow entry in the corresponding IP flow of the Fig.2.

[0050]

When the search processing section 16 searches the IP flow table 17, the encryption algorism is designated. Therefore, the packet processing section 14 determines that the packet belongs to the IP flow is an IPsec encrypting object packet. The packet is encapsulated by the packet of the IP destination address and the IP resource address designated by the IP flow table 17, then security data such as the encryption algorism is added to the encapsulated packet. After that, the packet processing section 14 transfers the encapsulated packet to the security processing section 19. (Step 603).

[0051]

The security processing section 19 separates the security data from the received packet. Then, the security processing section 19 transfers the packet to the packet processing section 14 again, after the IPsec encrypting process in accordance with the obtained security data (Step 604).

[0052]

The packet processing section 14 does not distinguishes the packet sent from the security processing section 19 from other packets received from the network interface, and carries out the searching operation of the IP flow table 17, handing with the normal packet (Step 605). At this time, the packet is already encapsulated to have the new IP destination address and the IP

source address. Therefore, the packet processing section 14 tentatively registers them as the new IP packet onto the IP flow table 17.

[0053]

After this, the microprocessor 11 carries out the routing process, and sends a searching result to the IP flow table 17 so as to formally register the IP flow entry (Step 606). As for the packet, the security process is never carried out again, because it is possible to determine that the security process is already carried out.

[0054]

The encrypted packet through the above mentioned processes are processed in the same manner as a normal packet (Refer to the Steps 313 to 315 and the steps 307 to 309 of Fig. 3).

Also, when the packet which has the same search key (the IP source address and the IP destination address) as the encrypted packet is received, the received packet can be encrypted by using the registered security data. This is because the IP flow corresponding to the received packet has been already registered onto the IP flow table 17. Therefore, as same as the omitting of the routing process for normal packet, there is no need for the microprocessor to gain the security data. As a result, the packet is sent to the security processing section 19 from the packet processing section 14 and the encryption can be carried out automatically.

[0055]

Next, a processing of the packet to the IPsec decryption will

be described with reference to Fig. 7. In this case, the microprocessor 11 extracts an SPI from the IPsec header of the packet, and searches the table for security process (Security Association Database) of the main memory 12, using the extracted SPI as a key. Thus, the microprocessor 11 gains an encrypting algorism and an encryption key (Step 701).

Further next, the microprocessor 11 sends the gained encrypting algorithm, encryption key and a physical port connected to the security processing section 19, to the IP flow table 17 through the search processing section 16. Thus, the tentatively registered IP flow entry is registered formally (Step 702).

[0056]

When the IP flow table 17 is searched by the search processing section 16 as for the packet which belongs to the IP flow, the packet processing section 14 determines that the packet is an IPsec decrypt object packet. This is because the encrypting algorithm is designated and the IP destination address is destined to the packet switching apparatus itself.

The security data such as the encrypting algorithm designated in the IP flow table 17 are added to the packet. Then, the packet is transferred to the security processing section 19 as designated destination. (Step 703).

[0057]

The security processing section 19 separates the security data from the received packet. Then, the security processing section 19 carries out the IPsec decrypting process for the received

packet in accordance with the gained data. Also, the security processing section 19 separates the packet from the encapsulated packet and transfers the packet to the packet processing section 14 again (Step 704).

[0058]

The packet processing section 14 does not distinguish the packet received from the security processing section 19 from the normal packets received from the external network interface. Thus, the searching of the IP flow table 17 is carried out handling as the normal packet (Step 705). At this time, the packet is decrypted to have an original IP destination address and an IP source address. Therefore, the packet processing section 14 tentatively registers the new IP flow of the packet onto the IP flow table 17.

[0059]

After this, the microprocessor 11 carries out the routing process to send the processing result to the IP flow table 17 so as to register the IP flow entry formally (Step 706). In this case, the security process is not carried out, because it is determined that the packet is destined to a host in a subnet of the packet switching apparatus itself.

[0060]

The packet passed through the above processing is handled in the same manner as the normal packet (Refer to the Steps 313 to 315 and Steps 307 to 309 of Fig. 3). Also, when a packet having the same search key (the IP source address and the IP destination address) as the decrypt object packet is received in

following steps, the decrypting process of the received packet can be carried out using the registered security data. This is because the corresponding IP flow is already registered onto the IP flow table 17. Therefore, as same as the omitting of the routing process for normal packet, there is no need for the microprocessor to gain the security data.

As a result, the packet is sent to the security processing section 19 from the packet processing section 14 and the decryption can be carried out automatically.

[0061]

The present invention is described up to this by the preferred embodiments. However, the present invention is not limited to the above embodiments.

[0062]

For example, in the above mentioned embodiments, the security process is carried out to the IPsec encrypting object packet by the security processing section 19, and then the encrypted packet is sent back to the packet processing section 14. At this time, the encrypted packet is handled as the normal packet by the packet processing section 14. Subsequently, the encrypted packet is transferred to the lower layer processing section 20.

However, the following processes may be carried out in place of above mentioned processes. That is, the packet processing section 14 encapsulates the IP packet and adds a data of the physical output port to the packet in addition to adding the MAC header and the security data. Then, the packet processing

section 14 transfers them to the security processing section 19.

The security processing section 19 stores the physical output port and the MAC header together with the packet. Then, the security processing section 19 carries out the IPsec packet encrypting process and then transfers the encrypted packet directly to the lower layer processing section 20 connected with the physical output port without passing through the packet processing section 14.

[0063]

In order to carry out the above mentioned processes, the processes of the present invention should be modified in the processing by the microprocessor 11 under the software control. That is, the routing process based on the IP destination address of the encapsulated IP packet are carried out together with the normal routing process at the same time, and the result of the routing process is registered on the IP flow table 17. Moreover, the processes in the packet processing section 14 and the security processing section 19 can be added as same as above mentioned operation so that realize the modified embodiment of the present invention.

[0064]

By this modified processes, the further improvement of throughput can be attained, compared with the process to the IPsec encrypting object packet shown in Fig. 6.

[0065]

Also, in the above embodiments, when the microprocessor 11 carries out the routing process to the packet belongs to the new

IP flow, the header section of the packet is copied from the processor processing queue of the packet memory 15 to the main memory 12.

However, replacing this process, the microprocessor 11 may receive an address pointer of the packet memory 15 indicating the header section and carry out the processes. That is, the packet itself is located in the packet memory 15 and the microprocessor 11 directly reads the header section of the packet through the processor bus 13 and the packet processing section 14.

[0066]

By the above mentioned modification, the number of times of packet data transferring can be reduced minimally so that the processing speed can be increased.

[0067]

Moreover, a crossbar switch may be adopted as the switch fabric 18. Basically in the packet data transfer of the above embodiment, a data transfer is carried out limitedly between the packet processing section 14 and one of the lower layer processing sections 20 or the security processing section 19.

However, as described above, when the packet transfer between the security processing section 19 and the lower layer processing section 20 is carried out, the frequency of data conflict is less in the crossbar switch so that the whole throughput can be improved.

[0068]

[Effect of the invention]

As described up to this, according to the packet switching apparatus of the present invention, once the routing process is carried out, the packet switching process can be achieved without further routing process by the microprocessor under the software control as for the packet having the same IP source address and IP destination address.

Therefore, the IP packet can be transferred at high speed.

[0069]

Also, the encrypting process and the decrypting process of the packet can be carried out in a hardware manner without using any process of the microprocessor. Therefore, the security process can be carried out at high speed.

[0070]

Also, a structure that transferring packet without the routing process of the microprocessor is realized by using the IP flow table is combined with the hardware for carrying out the security process. By this combination, the packet switching accompanied with the security process in the network layer can be carried out at very high speed, compared with the conventional packet switching apparatus.

[0071]

Moreover, the hardware for carrying out the security process is formed as one component of the switch fabric. Therefore, the independence of the security process can be improved. Thus, the addition of the security process to the packet switching apparatus and the addition or change of the encrypting system become easy. Therefore, the flexibility and the extendibility of

the packet switching apparatus can be improved.

[Brief Description of the drawings]

[Fig. 1]

Fig. 1 is a block diagram showing the structure of a packet switching apparatus according to an embodiment of the present invention;

[Fig. 2]

Fig. 2 is a diagram showing an example of an IP flow table in the embodiment;

[Fig. 3]

Fig. 3 is a flow chart showing a main flow of a packet process in the first embodiment;

[Fig. 4]

Fig. 4 is a flow chart showing a flow of a routing process in the embodiment;

[Fig. 5]

Figs. 5 is a flow chart and showing a flow of a packet process containing a security process in the embodiment and showing an operation in which a microprocessor acknowledges a kind of packets;

[Fig. 6]

Figs. 6 is flow chart showing a flow of a packet process containing a security process in the embodiment and showing a process for IPsec encrypting object packet;

[Fig. 7]

Figs. 7 is a flow chart showing a flow of a packet process containing a security process in the embodiment and showing a

process for IPsec encrypting object packet;

[Fig. 8]

Fig. 8 is a diagram showing the structure of an IP packet processed in an IPsec tunnel mode.

[Fig. 9]

Fig. 9 is a block diagram showing the structure of a conventional packet switching apparatus.

[Description of the reference Numerals and Symbols]

11 microprocessor

12 main memory

13 processor bus

14 packet processing section

15 packet memory

16 search processing section

17 IP flow table

18 switch fabric

19 security processing section

20 lower layer processing section

[Document Name] Abstract

[Abstract]

[Object]

Providing a packet switching apparatus which realizes the speed up of the packet switching process by reducing load of the microprocessor at the routing process and security process.

[Solving Means]

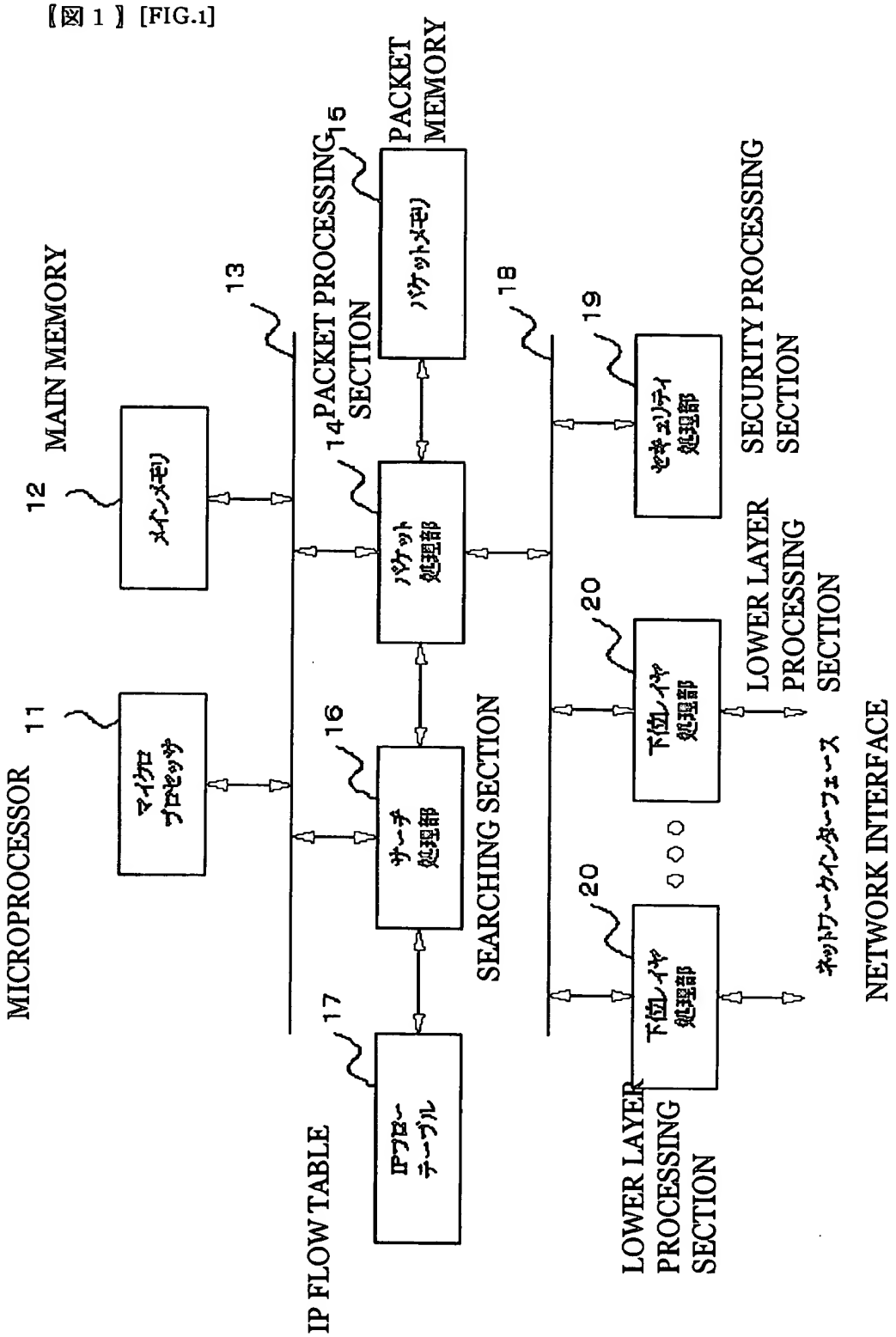
A packet switching apparatus which carries out a routing process in a packet unit and carries out a packet transferring, including a microprocessor which carries out routing process for a received packet under software program control; an IP flow table 17 which registers and stores a result of the routing process as for a packet to which the routing process is carried out by the microprocessor using an IP source address and an IP destination address as a search key; a means for packet process which searches the IP flow table using the IP source address and the IP destination address as a search key at receiving a packet, and which transfers the packet to an appropriate output port based on a result of a routing process indicated by the IP flow table without carrying out routing process by the microprocessor when a result of the searching indicates that a corresponding IP flow; a means for lower layer process which are connected to a network interface, and carries out a lower layer process for a received packet to be transferred to the means for packet process, and carries out a lower layer process for a received packet from the means for packet process to be outputted to a

network.

[Selected Drawing] Fig.1

【書類名】　図面　[DOCUMENT NAME] DRAWINGS

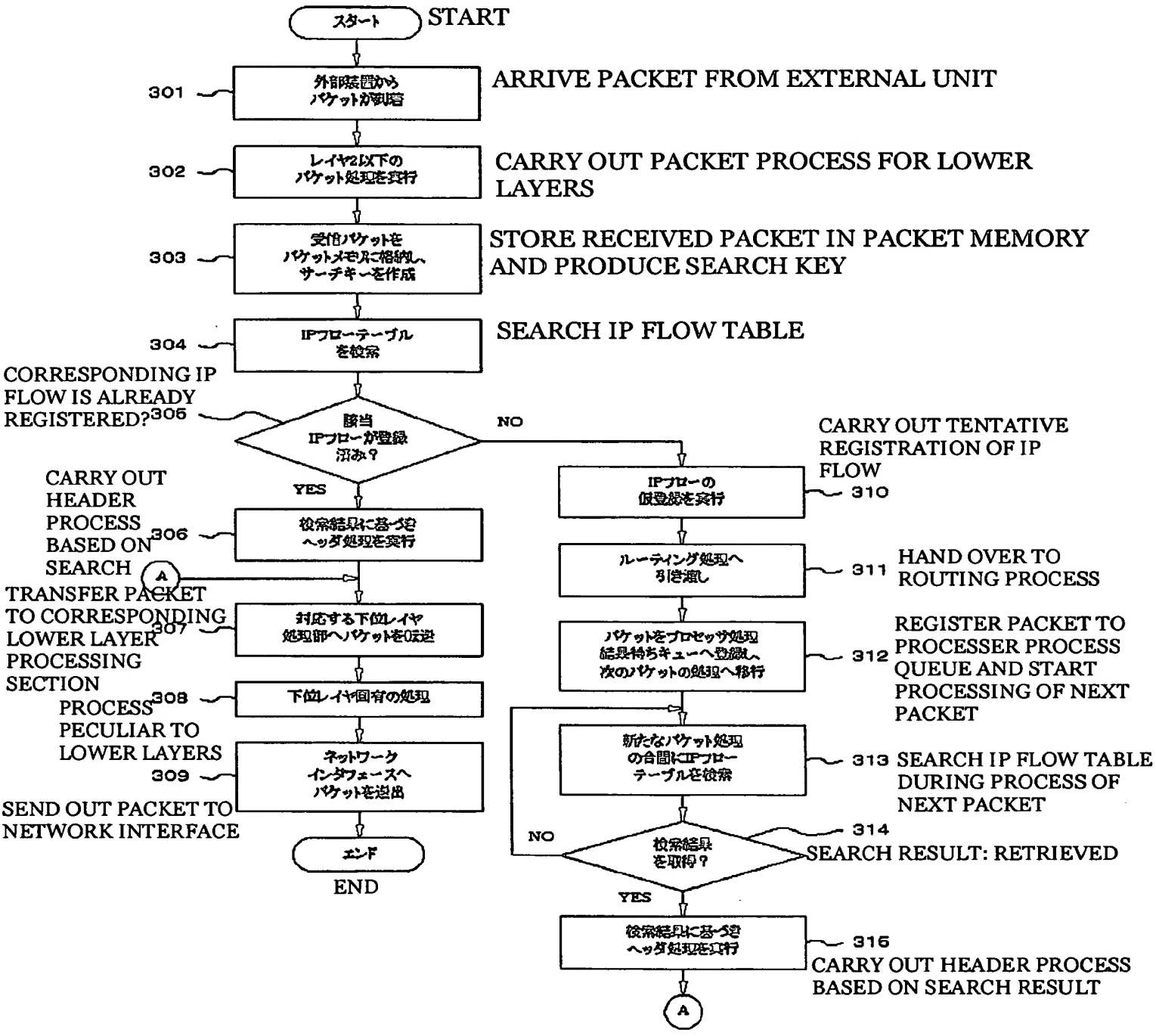
【図１】[FIG.1]



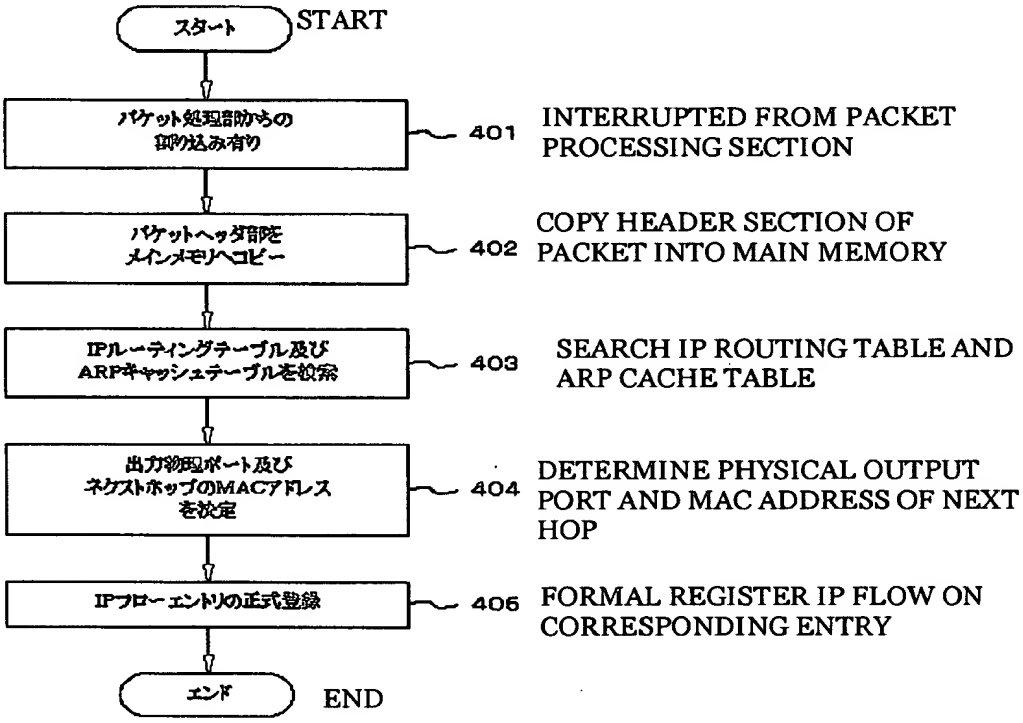
【図２】　[FIG.2]

SEARCH KEY サーチキー			ROUTING RESULT ルーティング結果			SECURITY DATA セキュリティ情報			
IP Source Address	IP Destination Address	MAC Source Address	MAC Destination Address	Output Port No.	Encryption Algorithm	Encryption Key	New IP Source Address	New IP Destination Address
AA BB CC DD	EE FF GG HH	123456	789012	2				
AA BB CC DD	KK LL MM NN			9	DES-CBC	XXXXXX	AA BB CC XX	KK LL MM YY
AA BB CC XX	KK LL MM YY	123456	789012	2				
KK LL MM YY	AA BB CC XX			9	DES-CBC	YYYYYY		
... ...	... ...	... ...	... ...	... ...	... ...	... ...	... ...	... ...

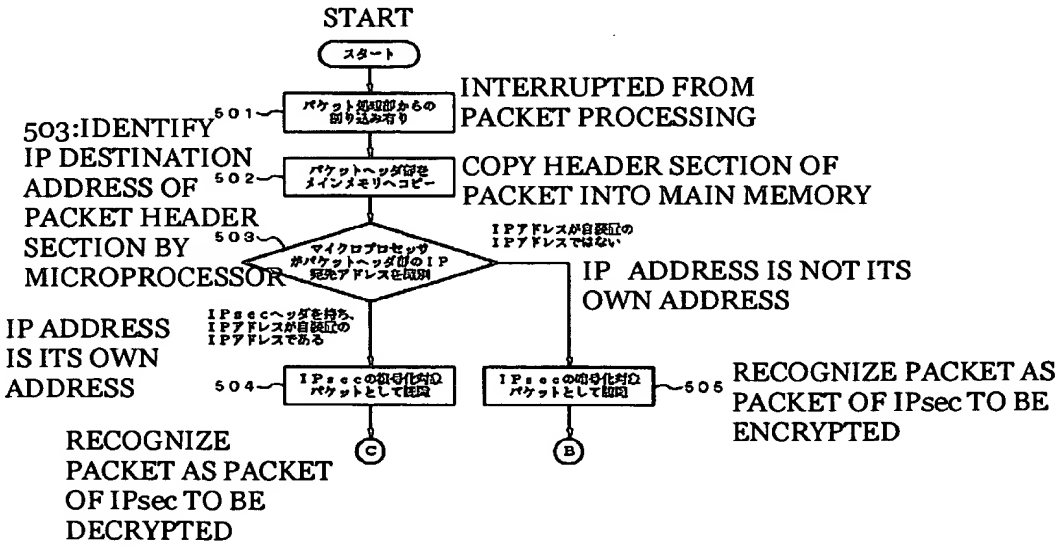
【図３】 [FIG.3]


スタート
START
外部装置から
パケットが到着
301
ARRIVE PACKET FROM EXTERNAL UNIT
レイヤ2以下の
パケット処理を実行
302
CARRY OUT PACKET PROCESS FOR LOWER LAYERS
受信パケットを
パケットメモリに格納し、
サーチキーを作成
303
STORE RECEIVED PACKET IN PACKET MEMORY AND PRODUCE SEARCH KEY
IPフローテーブル
を検索
304
SEARCH IP FLOW TABLE
該当
IPフローが登録
済み？
306
CORRESPONDING IP FLOW IS ALREADY REGISTERED?
NO
YES
CARRY OUT TENTATIVE REGISTRATION OF IP FLOW
IPフローの
仮登録を実行
310
ルーティング処理へ
引き渡し
311
HAND OVER TO ROUTING PROCESS
パケットをプロセッサ処理
結果待ちキューへ登録し、
次のパケットの処理へ移行
312
REGISTER PACKET TO PROCESSER PROCESS QUEUE AND START PROCESSING OF NEXT PACKET
新たなパケット処理
の合間にIPフロー
テーブルを検索
313
SEARCH IP FLOW TABLE DURING PROCESS OF NEXT PACKET
検索結果
を取得？
314
NO
SEARCH RESULT: RETRIEVED
YES
検索結果に基づき
ヘッダ処理を実行
316
CARRY OUT HEADER PROCESS BASED ON SEARCH RESULT
A
CARRY OUT HEADER PROCESS BASED ON SEARCH
306
A
TRANSFER PACKET TO CORRESPONDING LOWER LAYER PROCESSING SECTION
307
対応する下位レイヤ
処理部へパケットを転送
PROCESS PECULIAR TO LOWER LAYERS
308
下位レイヤ固有の処理
ネットワーク
インタフェースへ
パケットを送出
309
SEND OUT PACKET TO NETWORK INTERFACE
エンド
END

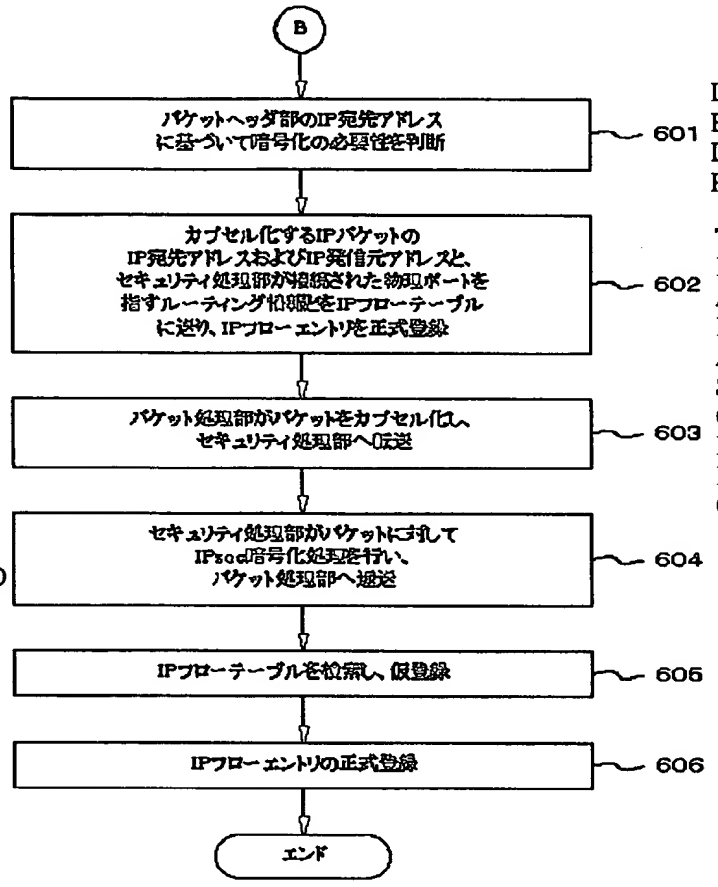
【図４】[FIG.4]



【図５】[FIG.5]



【図６】 [FIG.6]



END

DETERMINE NECESSITY OF ENCRYPTION BASED ON IP DESTINATION ADDRESS OF PACKET HEADER SECTION

TRANSFER TO IP FLOW TABLE, IP DESTINATION ADDRESS AND IP SOURCE ADDRESS OF IP PACKET TO BE CAPSULED AND ROUTING DATA SPECIFYING PHYSICAL PORT CONNECTED TO SECURITY PROCESSING SECTION, TO FORMAL REGISTER IP FLOW ON ENTRY

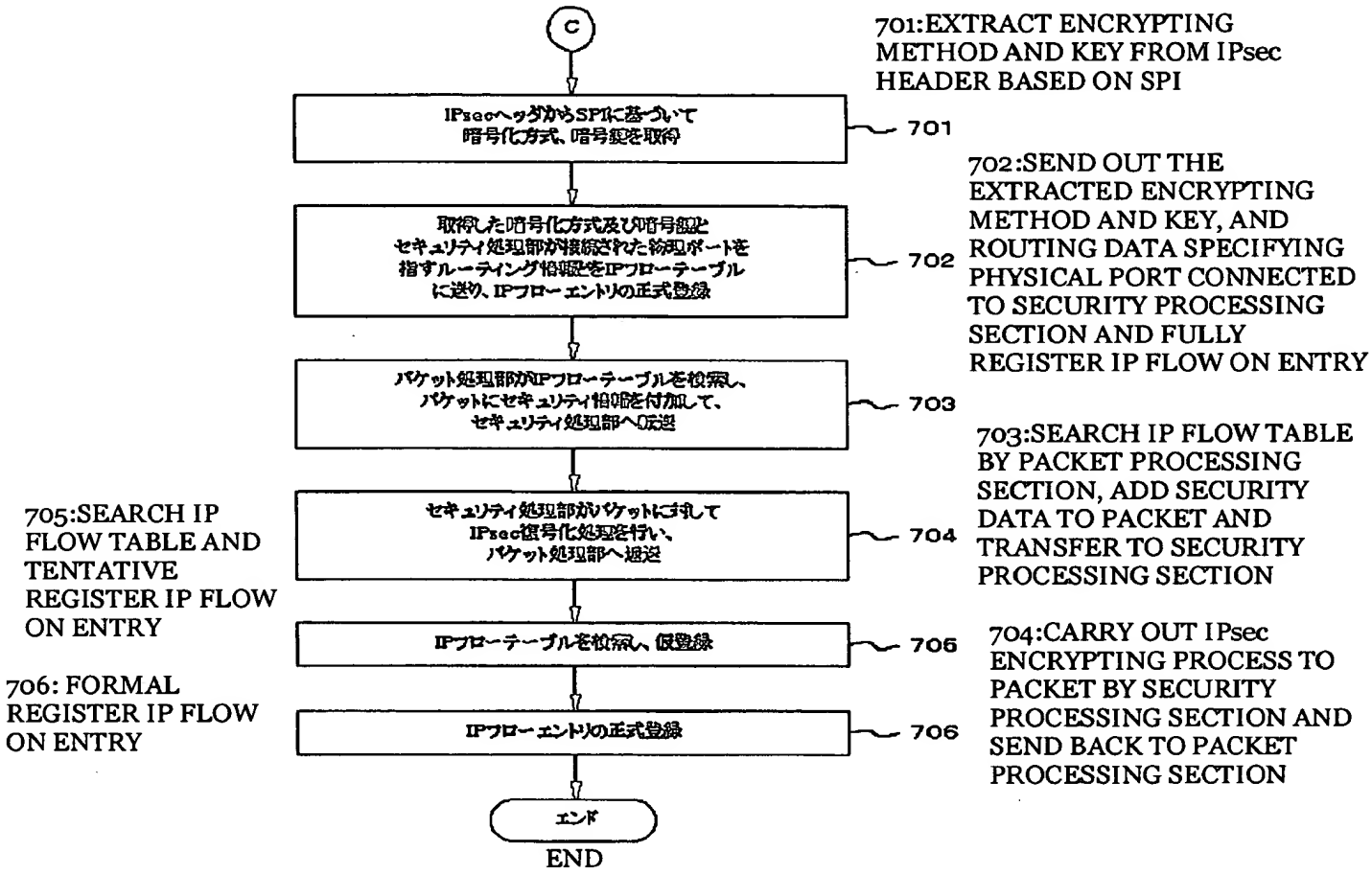
603:CAPSULATE PACKET BY PACKET PROCESSING SECTION AND TRANSFER TO SECURITY PROCESSING SECTION

604:CARRY OUT IPsec ENCRYPTING PROCESS TO PACKET BY SECURITY PROCESSING SECTION AND SEND BACK TO PACKET PROCESSING SECTION

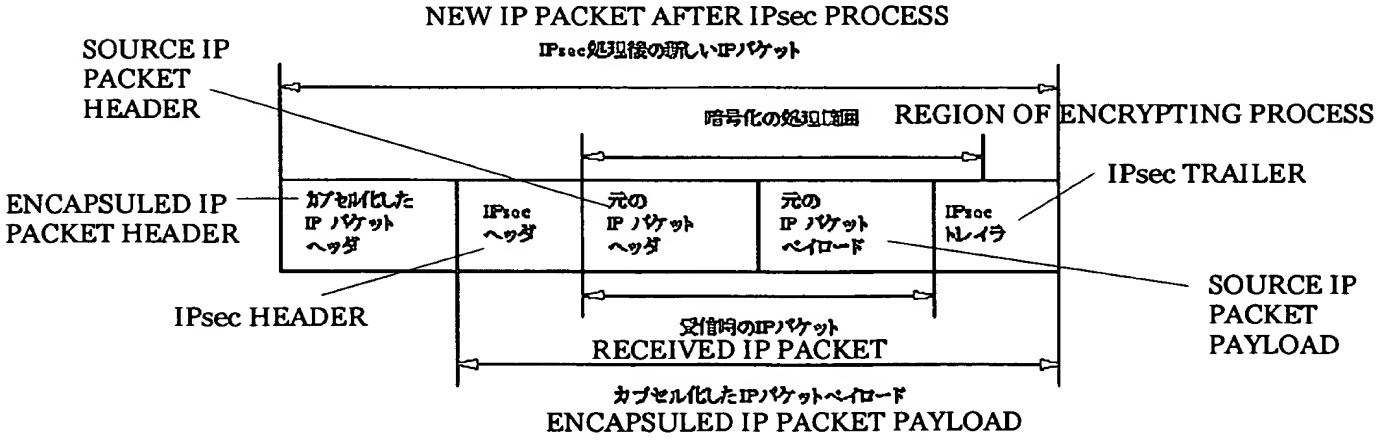
605:SEARCH IP FLOW TABLE AND TENTATIVE REGISTER ENTRY OF IP FLOW

606: FORMAL REGISTER IP FLOW ENTRY

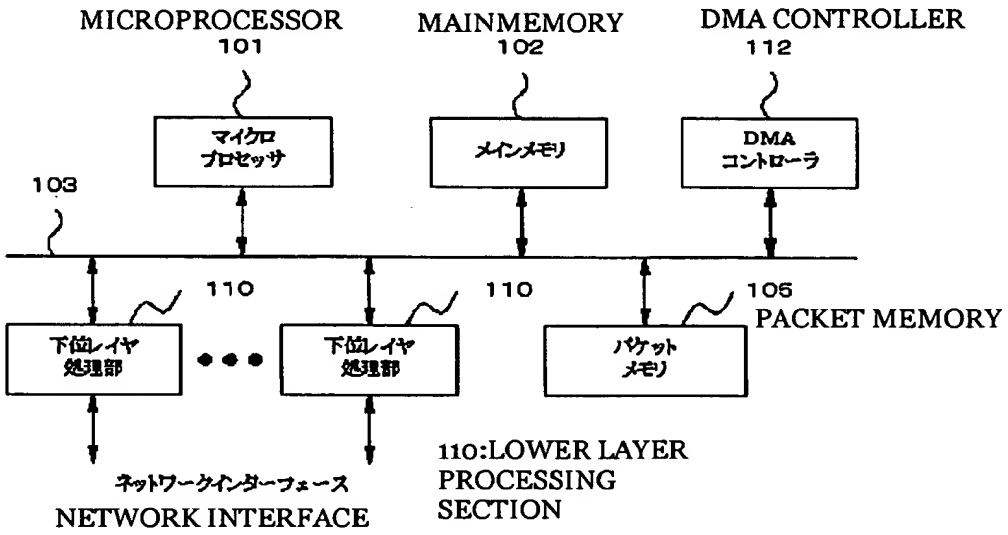
【図７】 [FIG.7]



【図８】 [FIG.8]



【図９】 [FIG.9]


MICROPROCESSOR
101
MAINMEMORY
102
DMA CONTROLLER
112
マイクロプロセッサ
メインメモリ
DMAコントローラ
103
110
110
105
PACKET MEMORY
下位レイヤ処理部
下位レイヤ処理部
パケットメモリ
ネットワークインターフェース
NETWORK INTERFACE
110:LOWER LAYER PROCESSING SECTION